DEPARTMENT OF THE NAVY
NAVAL MEDICAL RESEARCH CENTER DETACHMENT
LIMA, PERU
UNIT NUMBER 3800
APO AA 34041 - 3800

IN REPLY REFER TO

NMRCDINST 5500.1D
03 Mar 04

NMRCD INSTRUCTION 5500.1D

From: Officer-in-Charge

Subj: PHYSICAL SECURITY AND LOSS PREVENTION

Ref: (a) OPNAVINST 5530.14C
(b) SECNAVINST 5510.30A
(c) SECNAVINST 5510.13B

Encl: (1) Physical Security Plan (PSP)
(2) NMRCD Floor Wardens List

1. Purpose. To establish policy, provide guidance, and set forth standards for security measures to physically safeguard Navy property and material at this Detachment per references (a) through (c). Significant changes making this revision necessary include:

a. Identifying restricted areas and the minimum security measures required.

b. Assigning the chairperson of the training committee to make appropriate training record entries.

c. Re-establishing the Officer-in-Charge with the varied responsibilities in the event of bomb threats.

2 Cancellation NAMRIDINST 5500.1B

3. Scope. Enclosure (1) addresses the physical security and loss prevention responsibilities, physical security measures, and minimum criteria for physical security.

4. Background/Discussion. The provisions of this plan outline policy and provide guidance for security measures to physically safeguard Navy property and material. Department heads and personnel attached to this Detachment are responsible for taking these and any additional precautions to insure security and loss prevention.

5. Policy/Responsibility. Security is the direct, immediate, legal and moral responsibility of all persons in the naval service and civilians employed by the Department of the Navy.

a. The Officer-in-Charge is responsible for physical security and loss prevention within the Detachment.

b. The Security Officer shall be designated by the Officer-in-Charge in writing. He/she is responsible for planning, implementing, enforcing, and supervising the physical security loss prevention program of the Detachment.

6. Action. The Security Officer will establish and maintain a comprehensive physical security and loss prevention program per references (a) through (c).

7. Forms. The property Pass (NAVSUP Form 155) and the Special Request/Authorization (NAVPERS 1336/3) can both be obtained from the Administrative Department.

M. F. DAVID
Acting

PHYSYCAL SECURITY PLAN

(PSP)

NAVAL MEDICAL RESEARCH CENTER DETACHMENT
LIMA, PERU

Enclosure (1

PHYSICAL SECURITY PLAN
(PSP)

TABLE OF CONTENTS

CHAPTER 1

PHYSICAL SECURITY PLAN

1. Purpose. The physical Security Plan is part of the overall security program at the Naval Medical Medical Research Center Detachment, Lima, Peru (NMRCD). It is concerned with the means and measures designed to safeguard personnel and protect property by preventing, detecting, and confronting acts of unauthorized access, theft, pilferage, and any other acts which would reduce the capability of the activity to performs its mission.

2. Physical Security Surveys. Reference (a) directs that the Security Officer shall conduct a physical security survey at least annually using Appendix VIII of reference (a) as a guide. The survey shall be designed to show the Officer-in-Charge (OIC) what security measures are in effect, what areas need improvements, and to provide a basis for determining priorities for funding/work accomplishments. Results of the physical security surveys will be retained until completion of the cognizant Inspector General's command inspection or a minimum of two years, whichever is greater.

3. Security Areas. The Animal Containment Area located in the Annex/Animal Building shall be designated as a restricted access area. Entry way doors which provide entry into the individual containment suites shall be posted "Restricted Access Entry". Also posted on these portals shall be the biological hazard contained within that suite.

4. Responsibilities/Action. References (a) through (c) discuss general and detailed matters pertaining to responsibilities of all NMRCD personnel in the matter of physical security. All NMRCD personnel shall familiarize themselves with references (a) through (c) and are responsible for adherence to the regulations.

5. Physical Security Review Board. A physical security review board shall be established as per reference (a).

CHAPTER 2

COMPREHENSIVE LOSS PREVENTION PROGRAM (CLPP)

1. Purpose. To establish and promulgate the general policies and procedures for the conduct of loss prevention and loss reporting as per reference (a).

2. General. Loss and crime prevention are an all hands responsibility. A successful prevention program requires continuing command emphasis.

3. Responsibility. The Security Officer is responsible for the integration and development of NMRCD's CLPP with the U.S. Embassy-Peru and Centro Medico Naval.

a. The Security Officer shall maintain a close liaison with the Regional Security Office of the United States Embassy and the Security Office of the Centro Medico Naval, Peruvian Navy.

b. Department heads and supervisors are responsible for the security of personal property, equipment and spaces assigned to the department or to members of that department.

c. The Training Committee shall meet all training requirements as outlined in reference (a).

4. Loss Prevention. A vigorous analysis shall be done to help identify trends and patterns of losses. Loss property may prevent timely accomplishment of mission requirements. NMRCD's CLPP shall consist of:

a. Loss Analysis. A loss analysis shall be done to help identify trends and patterns of losses. All incidents involving reportable property must be included in an ongoing program of analysis.

b. Investigate and Police Resources. The ICASS agreement between the United States Embassy and NMRCD provides this Detachment with investigative and police resources.

c. Loss Prevention equipment. Exterior doors shall have locks as per reference (a).

d. Employee Education. All employees shall receive a security education briefing upon employment and annually thereafter. The Training Committee shall make appropriate entries in NMRCD's individual training records.

e. Discipline. Administrative personnel actions or action taken pursuant to the UCMJ are exclusive of actions by civilian authorities or litigation claims for the recovery of stolen property.

CHAPTER 3

MISSING, LOST, STOLEN, AND RECOVERED (MLSR) PROGRAM

1. Purpose. This program outlines the policy and procedures for reporting missing, lost, stolen, or recovered (MLSR) government property to proper authority as outlined in reference (a).

2. Background. The Department of the Navy has long recognized the importance of maintaining statistics to determine where, when, and how Navy property was missing, lost, or stolen. Based on this premise, MLSR instruction was initiated in 1973 with the ultimate goal of improving the Navy's physical security program and entering serialized property into a computer. Effective reporting of losses is basic to the determination of the scope of the loss prevention program which must be developed by the command. When reviewing property losses which are not critical to national security and which do not threaten the civilian population, it is of primary importance to know whether the expenditure of funds on physical security will net a payback in loss reduction. If real losses are extremely low, and involve only non-sensitive, low value, or non-hazardous materials, it may be more cost-effective to absorb such losses. Nevertheless, actual losses must be reported so that an accurate decision can be made by the command.

3. Action. NMRCD personnel shall report MLSR incidents to the Security Officer. The Security officer will investigate the incident and decide if further action is warranted as directed by reference (a) and reference (c).

CHAPTER 4

KEY CONTROL PROGRAM

1. Purpose. Reference (a) directs that each naval activity must establish a strict key and lock control program. Included within this program are all keys, locks, padlocks, and locking devices used to protect or secure restricted areas and activity perimeters.

2. Key Control Officer. The Facilities Manager shall be the Key Control Officer and be designated in writing by the OIC. The duties of the key control officer shall include:

a. Maintain all non-issued keys in a central security container that conforms to standards outlined in reference (c)

b. Maintain a key control register

c. Conduct an annual inventory of all issued keys

d. Develop a system with records showing positive key and lock accountability.

e. Approval of all locks and padlocks for meeting minimum military specification.

CHAPTER 5

EMPLOYEE SECURITY EDUCATION PROGRAM

1. Purpose. A security education program shall be established at this Detachment to ensure that all assigned personnel, military and civilian, recognize, understand and carry out their responsibility regarding security. Any security program or system designed to combat the security threats outlined in reference (a) will be ineffective unless it is supported by a comprehensive security education program.

2. Action. The Training Committee, in cooperation with the Security Officer and the Security Manager shall develop a training program that encourages prompt reporting of security breaches and attempt to:

a. Reduce security infractions and violations

b. Act as communication feedback for improved protective measures.

c. Reduce losses of government property.

d. Reduce vulnerability

e. Instill security consciousness, which will solicit potential threat information.

The security education program, shall include lectures from the Regional Security Office of the United States Embassy and include posters, placards, and leaflets.

3. Indocrination. The Security Officer is responsible for the indocrination of all newly arriving NMRCD personnel. The security indocrination shall include:

a. A general orientation on the need for and dangers to security.

b. The individual's responsibility in preventing infractions.

c The dangers of loose talk and operational carelessness.

d. Define general security measures such as Centro Medico Naval pass and ID requirements, POV control and automobile inspection, and the removal of government property from the station.

CHAPTER 6

CLASSIFIED MATERIAL

1. Classified Material. The transport to or the storage at NMRCD of any form of classified material is prohibited until further notice. Personnel designated to pick up message traffic at the Communications Center, The United States Embassy are to check and remove for content and then properly destroy in the nearby shredder provided for this purpose.

2. Review. The Officer-in-Charge and the Security Officer will periodically conduct a review of this plan.

CHAPTER 7

OPERATIONS SECURITY (OPSEC) PLAN

1 Purpose. To establish an operations security plan for NMRCD

2. Scope. The provisions set forth in this plan apply to all NMRCD personnel.

3. Structure.

a. The organizational element responsible for OPSEC shall be composed of the following:

Officer-in-Charge

Administrative Officer

b. The responsibilities of this element in implementing the OPSEC program are as follows:

(1) Officer-in-Charge - direction and oversight for the OPSEC command element.

(2) Administrative Officer - implements the program and provides specific guidance to the Officer-in-Charge.

4. Training.

a. OPSEC Orientation Training. All personnel coming into NMRCD will receive this training from the security manager as part of the information/personnel/OPSEC awareness briefing at indocrination.

b. Continuing Awareness OPSEC awareness shall be maintained by:

(1) Conducting the OPSEC awareness briefing yearly as part of scheduled general military training.

(2) Performing OPSEC surveys and special operations as necessary.

(3) Using available posters and plan of the day notices to reinforce employee awareness.

OPSEC INDOCRINATION

The Information and Personnel Security Program will ensure compliance with references (a) through (c) and make sure information classified under authority of Executive Order 12356 of April 2, 1982 is protected form unauthorized disclosure. Additionally, this program will ensure that the appointment or retention of civilian employees, acceptance or retention of military personnel, granting access to classified information because of rank, position or level of security clearance. Access to classified information will be controlled on a "need to know" basis.

1. Responsibilities.

a. Officer-In-Charge. The Officer-In-Charge (OIC) is responsible for effectively carrying out the information and personnel security program at NMRCD. The OIC has the overall responsibility for safeguarding all classified information and instructing personnel security practices and procedures. The OIC is the ultimate authority for granting security clearances and is responsible for setting up a program for continuous evaluation of eligibility for access to classified information.

b. Command Security Officer. The Security Officer is appointed, in writing, by the OIC. He/she is the primary contact for information and personnel security at NMRCD and is responsible to the OIC for managing the program.

e. All Hands. Effective security education program is to ensure that all NMRCD personnel understand the means available to safeguard classified material. All personnel will receive the requisite security training, regardless of their access to classified information.

2. Security Education

a. The purpose of the security education program is to ensure that all NMRCD personnel understand the means available to safeguard classified material. All personnel will receive the requisite security training, regardless of their access to classified information.

b. The following are the minimum requirements for security

education to be given at NMRCD:

(1) Indocrination for all hands in basic security principles. (Delivered as an informal lecture by the Security Officer at the time of check-in to NMRCD for duty).

(2) Security orientation for those who will have access to classified information at the time of assignment. Special handling instructions, safeguards, laws, and regulations are made clear to new custodians, managers and clerks at the time of assignment and turnover to these positions will be covered.

(3) On-the-job training (OJT) in specific security requirements for the duties assigned. The Security Officer and the Security Manager receive OJT on maintenance of the classified material log, operation of the safe, and filing of classified materials.

(4) Annual refresher briefings for those who have access to classified information. Annual refresher training is provided by scheduled general military training (GMT) classes several times a year. The training provided by GMT instructors or guest speakers from the Regional Security Office, United States Embassy.

(5) Counter-espionage briefings once every two years for those who have access to information classified SECRET or above.

(6) Special briefings as circumstances dictate

(7) Debriefing at the time a Security Termination Statement, OPNAV Form 5511/14, is prepared.

3. Security Investigations. No one will be granted clearance, given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made of his or her loyalty, reliability and trustworthiness. The first determination will be based on the minimum personnel security investigation (PSI) for the level of clearance needed. Before starting the PSI, The Security Officer will first make sure a valid investigation has not already been completed, and that locally available records (personnel, medical, legal, security, base security and other command records) do not have information which show the person is not a good candidate for a position of

trust. When it is decided that a PSI is needed, the Security Officer will help the person in completing the forms required by reference (b). Satisfactory completion of the PSI will serve as the basis for granting a final security clearance. The PSI will be recorded by the Security Officer in Part II - "Record of Investigation" on the Certificate of Personnel Security Investigation, Clearance, and Access, OPNAV Form 5520/20.

4. Security Clearance and Access

a. Interim Clearance. An interim clearance for the level of access needed may be granted for a period of six months if a PSI has been requested and a review of locally available records is favorable. The review of local civilian law enforcement records, or the National Crime Information Center (NCIC) records, is prohibited. A review of records at the local Naval Investigative Service is also inappropriate. Interim clearances for military personnel may be extended in six-month increments if the PSI is not finished by the expiration date and tracer action confirms the PSI is still open. Interim clearances for civilian personnel will be extended only with the approval of Department of the Navy Central Adjudication Facility (CAF).

b. Final Clearance. When the results of a PSI are received, the Officer-In-Charge may grant a final clearance for the level of access needed to perform assigned duties. Security clearances will be recorded in Part III, the "Record of Clearance" OPNAV Form 5520/20. When a clearance is denied, the OIC will enter "DENIED" in Part III and explain in the "Comments" section. The explanation, signed by the Officer-In-Charge, will not specify the cause for denial, but will refer to the personnel record entry, command correspondence or other documentation supporting the action.

c. Access. The OIC may grant access to classified information to people who have an official need-to-know and a valid security clearance. Granting access will take place only after the individual has read and signed a Classified Information Nondisclosure Agreement (SF 312). If a member has previously signed an SF 189, SF 312 is not needed as the SF 189 will be for continuously evaluating personnel eligibility for access to classified information. The access will be recorded in part IV "Record of Access" of OPNAV Form 5520/20. Access is automatically terminated when the person transfers from the command, is discharged, or is separated from Federal Service. When a

clearance is administratively withdrawn, or revoked for cause, the access based on the clearance is canceled. Special access programs will be handled per reference (b) sections (1-5) and (12-2).

d. Adjustment/Termination of Clearance and Access

(1) When there is no longer a need for access to a particular level of classified material, the clearance is withdrawn, the Security Officer will overwrite the clearance entry with, "WITHDRAWN", in Part III OPNAV Form 5520/20, and the "Comments" section must be annotated to show the action was taken administratively, with no prejudice to the individual's future eligibility for access to classified material. Access will be adjusted to reflect current need.

(2) When a clearance is revoked for cause, the Security Officer will overwrite the clearance entry with, "REVOKED", in Part III of OPNAV Form 5520/20, and explain in the "Comments" section. The explanation, signed by the OIC, will not specify the cause for revocation, but will refer to the personnel record entry, command correspondence, or other documentation supporting the action.

(3) When the clearance and access have been reduced or terminated, the person will be debriefed.

5. Telephone Security. All telephones at NMRCD are non-secure. Therefore, discussing or transmitting classified information over the telephone is strictly prohibited. NMRCD telephones are subject to communications security monitoring at all times and are provided for the transmission of official government business only.

6. Reports of loss, compromise, or possible compromise of classified material will be turned over to the Security Officer for review and action. The Security Officer will keep the OIC informed at all times of any incidents, reports, and actions required concerning such matters.

7. Security violations not resulting in compromise or loss will be handled in accordance with OPNAVINST 5510.1 chapter 4, section 13.

8. Visit Control

a. General visiting will be allowed only to authorized areas. The animal containment area will be placed off-limits to all visitors unless specifically authorized by the OIC or the Security Officer. The movement of all visitors throughout NMRCD will be restricted. A visitor is any person who is not permanently attached nor employed by NMRCD, including persons on temporary additional duty (TAD).

b. All visitors will be required to check in and out at the reception desk located at the primary entrance to the main building. All visitors must undergo a cursory inspection of any bags or containers in their possession by the assigned security guard. Visitors will be required to show and present proper identification to the receptionist. Their identification papers will be held by the receptionist and in their place a "Temporary visitor" badge will be handed out and visibly worn at all times. Upon departure from NMRCD the visitor will turn over the temporary visitor badge and receive their identification documents.

c. Individuals wishing access to NMRCD must obtain a sponsor who can apply for a visitor entry request. The visitor entry request allows for entry onto the Centro Medico Naval compound. A NMCD sponsor can be any individual who is permanently assigned or employed at NMRCD.

d. Visitors, who must conduct their business beyond the reception desk area, will be escorted by their sponsor or sponsoring department at all times. No visitor will be left unattended and allowed to move about the Detachment unescorted

e. Visitors found in areas without an escort or wandering around the facility by staff or security personnel will be returned to the reception desk area for questioning by the security personnel. The sponsor will be contacted and a determination will be made whether or not to terminate access to NMRCD at this time.

f. Violations by visitors accessing NMRCD will be handled and investigated by the Security Officer. Further actions to deny visitation to NMCD temporarily or permanently will be made by the Security Officer and the Officer-In-Charge. The Officer-In-Charge or the Security Officer may suspend temporarily or permanently the

ability for any staff individual to sponsor visitor access to NMRCD.

CHAPTER 8

BOMB THREAT PROCEDURES

1. Purpose. To provide outline guidance in planning for or responding to bomb threats. Bomb threat planning is an important facet of any physical security program (plan), whether for single buildings, a facility, or an installation.

2 Definitions.

a. A bomb is a device capable of producing damage to material and injury or death to personnel when detonated or ignited. Bombs are classified as explosive or incendiary. An explosive bomb causes damage by fragmentation, heat, and blast wave. The heat produced often causes a secondary substantial explosion when ignited. Bombing occurs when an explosive bomb detonates or an incendiary bomb ignites.

b. A bomb threat is a message delivered by means which may or may not:

(1) Specify location of the bomb.
(2) Include the time for detonation/ignition.
(3) Contain an ultimatum related to the detonation ignition or concealment of a bomb.

c. A bomb incident involves any occurrence concerning the detonation or ignition of a bomb, the discovery of a bomb, or receipt of a bomb threat.

3. Responsibilities.

a. Security Officer. The Security Officer is responsible to the Officer-In-Charge for ensuring that appropriate procedures are implemented concerning bomb threat incidents.

b. The Officer-in-Charge, or the Security Officer shall report threatening calls or notices to the Regional Security Office, United States Embassy and the Security Office of the Centro Medico Naval, Peruvian Navy and generate required SITREP/OPREP message traffic related to the incident. Appendix A shall be included in the command logbook and training programs.

c. Staff Personnel. Staff personnel shall be familiar with Appendix A and, upon receipt of a bomb threat activate the bomb threat notification checklist and call the Security Officer or the Officer-In-Charge, RSO U.S. Embassy and the Security Office, Centro Medico Naval.

d. Command Duty Officer (CDO). The CDO, or in his/her absence the Security Officer, shall evacuate the threatened area until deemed safe to return by Base Security (CMN) or the RSO, U.S. Embassy. Precautions must be taken to avoid panic and confusion, and personnel evacuated shall be kept at least 300 fe from the threatened area.

NOTE: Radio communications will not be used Within 150 feet of the threatened area because Of the possibility of detonating an electric Blasting cap by radio transmissions. This Includes the small hand radios used by police Security personnel. The same prohibition must be applied to sirens on emergency vehicles.

4. Subject to the orders of the Officer-In-Charge, the Command Duty Officer or the Security Officer shall exercise undisputed control of evacuation and search procedures and will complete all required reports. The CDO or SO must also verify that all personnel identified on the bomb threat notification checklist ar notified.

5. Searches shall be thorough and well coordinated, and shall cove all spaces where an explosive object might be placed. The search will not commence until at least 30 minutes after detonation time, if time is provided by the caller. If a time is not provided, the search should commence as soon as evacuation is complete. If the area is not evacuated, the search should commence as soon as evacuation is complete. If the area is not evacuated, the search should commence when reasonable attempts have been completed for the protection of life and property. Whe possible, a bomb detection dog team should be utilized.

6. A search party should include personnel who are familiar with the building or area to be searched. Personnel used in search party should be familiar enough with the area to spot unusual condition, foreign objects, etc.

7. If appropriate, search personnel shall be divided into teams. Team leaders will be identified and instructed to report their findings directly to the CDO. Searches shall be conducted systematically, being careful to examine all rooms and spaces. The search of the outside of a building is more important because this is the most accessible area to the bomber. The search should be conducted to a distance of 25 to 50 feet from the building, outward. Search personnel should not smoke or ignite any type of incendiary material in the threatened area.

8. Searchers must assume that any suspected explosive device package, bomb, or foreign object is dangerous and must not be handled in any way. They shall not touch or disturb any device or object found during the search. Suspected objects or devices will be examined and/or removed only by authorized explosive ordnance disposal (EOD) personnel.

9. In instances where the evacuation of a threatened area is considered inappropriate, the area shall be searched to the satisfaction of the CDO by personnel working or on duty in the area. If suspected explosive devices are found, the area will be evacuated.

10. In instances when the threatened area is evacuated, security personnel shall be employed around the area for traffic control and to prevent the entry of all unauthorized personnel. In searching for explosive devices, except for the most unusual circumstances, EOD personnel and military/security police WILL NOT be used to search for reported explosive devices. Rather, such searches will be conducted by designated individuals familiar with the area and its contents.

11. Fire, medical, and other available rescue personnel should be alerted and placed on standby to render aid if necessary. Fuel lines into the area should be interrupted and all flammable material in the area should be removed if possible.

12. The preservation of life is paramount and takes precedence over any other action contemplated. Extreme caution should be exercised at all times. Crowds hinder search and rescue operations and must be constantly controlled.

13. Threatened or bombed areas must be carefully inspected, evaluated, and declared safe by the Security Officer before entry

into the area is authorized. Prior to authorizing re-entry into threatened area, Security Officer or OIC will collaborate with either agents of the RSO, U.S. Embassy or Security Office, Centro Medico Naval, Peruvian Navy to ensure proper protection of the crime scene. Investigative personnel, EOD, and fire department personnel must be allowed access to the threatened area at any time.

14. SITREP and OPREP-3 reports will be submitted by the OIC or Security Officer per reference (a). Any known "Hoax" bomb threat reported will be limited to SITREPS.

15. All bomb threats should be treated as bona-fide. Risks and possible consequences are too great to regard them as hoaxes.

16. Telephone Procedure for Bomb Threat. See Appendix A.

17. Action to Take After Call:

a. Notify the OIC, Security Officer or CDO immediately. Then notify RSO, U.S. Embassy and the Security Office at Centro Medico Naval, Peruvian Navy.

b. Refer to notification check list

CHAPTER 9

COUNTERSABOTAGE PLAN

1. Purpose. To establish a countersabotage plan

2. Scope. The provisions of this plan apply to all NMRCD personnel. Nothing herein should be construed to nullify directives issued by a higher authority

3. General. Sabotage is an act or acts with intent to injure, interfere with or obstruct the national defense or a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. By mere virtue of description, there are infinite possibilities for sabotage activities. The following guidelines may be used in whole or in part to report and control actual or suspected sabotage attempts.

> NOTE: During peace time, destruction of government property by military and/or civilian personnel, is normally investigated by the Naval Investigate Service (NIS) as an act of wrongful Destruction vice sabotage.

4. Reporting Sabotage. Recognition of an act of sabotage is often difficult. Some acts of sabotage are obvious; i.e., bomb planted in the pesticide storage area, subversive literature left in the lounge, etc. Some acts are not obvious; i.e., small piece of metal in a moving gear, fire in the warehouse. Due to difficulty of recognizing sabotage acts, all suspected acts of sabotage shall be reported. The observer will contact the OIC or the Security Officer and report as follows:

a. Give the name of the saboteur, if known, and location and description of sabotage act.

b. Leave his/her name and telephone number investigative purposes.

5. Reporting Procedure. After the person has contacted the Security Officer and the CDO, the Security Officer will take charge of the area and then notify the following personnel:

a. Officer-in-Charge

b. Administrative Officer

6. Parcel Inspection. As part of the counter-sabotage, counter-espionage, anti-terrorist threat (Threatcons) effort and loss prevention program, the Physical Security Officer is authorized to conduct administrative cursory inspections of all hand-carried parcels entering or leaving spaces and NMRCD. Body searches, pat downs, etc., are not authorized.

a. Parcels, for the purpose of this instruction, include handbags, purses, briefcases, display cases, luggage, lunch boxes tool kits, boxes, bags, etc.

b. The Security Officer will ensure that parcel inspections are conducted without regard to sex, rank, grade, rate, race or military/civilian status of the individual possessing the parcel(s).

c. The Security Officer will not confiscate any suspect or suspicious item(s), but will request that the individual(s), after notifying the OIC, remain until either the RSO, U.S. Embassy or the Security Office personnel of the Centro Medico Naval arrive and investigate the situation.

7. Miscellaneous. The best countermeasures against sabotage act(s) is employee education, planning and awareness. It is imperative that all employees, military and civilian, be aware that saboteur activities can happen and they should be prepared to react immediately. Remember, any unusual act by any person, can be an act of sabotage.

CHAPTER 10

NMRCD DEFENSE PLAN

1. Purpose. To provide instructions to prevent personal injuries to personnel and/or damage to government property in NMRCD in case of civil unrest which may result in a hostile demonstration and an unauthorized intrusion of the building.

2. Applicability. All building occupants must become familiar and comply with these procedures. Each of us must be prepared for such an emergency.

3. Responsibilities. The Security Officer (NMRCD Administrative Officer) is responsible for the design, implementation and dissemination of instructions regarding this emergency situation and the use of secured areas within each floor in the NMRCD facility. There are Floor Wardens and Alternate Floor Wardens designated to assist the Security Officer (SO) in the preparation and implementation of appropriate emergency actions. In general, all NMRCD occupants must be prepared to take over the Floor Wardens' responsibility during this emergency in his/her absence.

4. Procedures.

a. FIRST STAGE

(1) As soon as the SO is informed and/or the NMRCD guards observe an unusual large number of demonstrators gathering in the neighborhood of the NMRCD facility, they will inform the SO.

(2) The SO and/or the senior guard on duty in turn will inform the Officer in Charge and the RSO by phone or any other means of communication available about the situation immediately.

(3) Likewise, the senior guard on duty will inform COSMOS about the situation through his own command channels.

(4) The USO will do a quick assessment of the situation in order to make proper decisions.

(5) If the situation warrants it, emergency procedures will be initiated.

b. SECOND STAGE

(1) After consulting with the RSO, the Officer-in-Charge will notify the USO on how to proceed and verbal instructions will be provided through the Selectone system. Note: Priority will be given to releasing non-essential personnel prior to the situation metastasis. If necessary, the SO will contact appropriate Centro Medico Naval Base personnel for reinforcements (i.e., armed military police officers).

(2) The NMRCD guards (Static and Rover) will close all external gates and ensure that all hardline doors are secured. Moreover, they will remain alert to the developing situation.

(3) The SO will remain in the NMRCD facility until the emergency is over.

(4) The Floor Wardens will visually ensure that all external doors are secured.

(5) Employees, guided by the Floor Wardens, will turn off all light features and proceed to the eastern or southern end of their floor, away from the windows.

(6) Each Floor Warden should count his/her personnel in the floor, making sure that everybody is inside and then report to the Security Officer.

(7) Employees are expected to remain calm and alert for further instructions, which will be given through the Selectone system.

(8) Emergency team members (first aid and damage control) must remain alert in case a fire starts, caused by Molotov bombs thrown at the building, or if an employee becomes panicky.

(10) Upon receiving full reports from the Floor Wardens the SO will call the RSO through the MSG Post 1 and give a complete report about the situation.

(11) The RSO will inform the COM regarding the situation and make a recommendation (based on the advice of the USO and the Officer in Charge) to have all remaining NMRCD personnel remain in place or relocate them to another building on the base. If personnel relocate to another building on the base, then they will be instructed in accordance with NMRCD's Internal Defense Plan.

Appendix A

BOMB THREAT NOTIFICATION CHECK LIST

1. Instructions. After receiving a bomb threat and recording the information, first notify the Officer-in-Charge, Administrative Officer, or the Security Officer, then activate the bomb threat notification check list by contacting the following:

a. Affected Department head
b. Base Security Office
c. Base Fire Department
d. RSO, U.S. Embassy, ext. 7334.

2. The person receiving the call will ensure all of the above are notified and are provided with the following information:

a. Time call received.
b. Location of bomb, if given.
c. Room number (if available).
d. Human target (if available)

3. Exterior search. Make visual inspection of the surrounding area, noting anything unusual. After a brief visual inspection, start a step-by-step inspection of the building(s):

EXTERIOR SEARCH LIST

SPACE	CHECKED BY
LAWN:	
PARKET VEHICULES:	
UTILITY POLES:	
DRAINAGE SYSTEMS:	
SHURBS:	
GENERATOR ROOM(S):	
BASEMENT/GARAGE:	
WINDOWS:	

DOORS:

ANIMAL PENS:

PATIO AREAS:

ROOF TOP

4. Interior Search. This should be a thorough, well-planned operation with a designated individual coordinating all search parties. Start search at bottom of the building and search toward the top, checking each floor in sequence.

INTERIOR SEARCH CHECKLIST

SPACE	CHECKED BY
OFFICE/ADMIN SPACES:	
CONFERENCE ROOM:	
RECEIPTION DESK/AREA:	
BACTERIOLOGY LABORATORY:	
ENTOMOLOGY LABORATORY:	
MEDIA PREPARATION AREA:	
PARASITOLOGY LABORATOTY:	
SEROLOGY LABORATORY:	
STERILIZATION ROOM:	
RECEIVING AREA:	
ELEVATOR & SHAFT:	
SPECIMEN RECEIVING LAB:	
REST ROOMS, FIRST FLOOR:	
LOUNGE/LUNCH AREA:	

REST ROOMS, SECOND FLOOR:

DATA CENTER:

LIBRARY & STORAGES AREA:

MEDICAL REPAIR AREA

SUPPLY & STORAGE AREAS

5. If a suspicious object is found during the search, secure that area and report the item to the Security Officer. The report should include:

a. Location.
b. Description
   (1) Size
   (2) Shape
   (3) Any noises

6. If detailed search has been conducted with no devices located, secure the search.

PRECAUTIONS TO BE OBSERVED WITH SUSPECTED BOMBS

1. While some of the following precautions may seem elementary none should be taken for granted.

a. DON'T cut a string

b. DON'T shake a bomb. Some contacts are arranged with Mercury switches and the shaking of the bomb will cause the circuit to be completed. Other contacts are made with a very fine space separating them and shaking of the bomb may cause ignition.

c. DON'T indiscriminately shock or jar the bomb.

d. DON'T handle the package unnecessarily

e. DON'T touch a bomb unless you are duty bound to do so

f. DON'T smoke in the immediate vicinity of the suspected bomb.

g. DON'T accept identification markings as legitimate.

h. DON'T take for granted the identification of the markings On the package, as they may be forged. Keep in mind that bombs are usually camouflaged in order to throw the recipient off his guard.

i. DON'T take for granted that the package is bona fide because of its having been sent through the mail. Many bombs are forwarded in this manner. Others are sent through express agencies, while some are delivered by individual messengers.

j. DON'T open suspicious packages

k. Clear unnecessary personnel out of the vicinity of a suspected bomb.

NMRCD FLOOR WARDENS LIST

Building # 1

First floor: LCDR Mary David / Rina Meza

Second floor: Miguel Ramirez / Carolina Guevara

Building # 2

First floor: Rickey Luckett / Milagros Salazar

Second floor: Zoe Moran / Gloria Chauca

Mustering Officers:

Mariana Garcia

Gloria Talledo

Sayda Chavez

Enclosure (2)